AMENDMENT TO THE CLAIMS

1-18 (Cancelled)

19. (New) A computer-implemented process comprising:

obtaining a set of one or more private values $Q_1, Q_2, \ldots, Q_m$ and respective public values $G_1, G_2, \ldots, G_m$, each pair of keys (Q_i, G_i) verifying either the equation $G_i \cdot Q_i^v \equiv 1 \bmod n$ or the equation $G_i \equiv Q_i^v \bmod n$, wherein m is an integer greater than or equal to 1, i is an integer between 1 and m, and wherein n is a public integer equal to the product of f private prime factors designated by $p_1, \ldots, p_f$, at least two of these prime factors being different from each other, wherein f is an integer greater than 1, and wherein v is a public exponent such that $v = 2^k$, wherein k is a security parameter having an integer value greater than 1, and wherein each public value G_i (for $i = 1, \ldots, m$) is such that $G_i \equiv g_i^2 \bmod n$, wherein g_i (for $i = 1, \ldots, m$) is a base number having an integer value greater than 1 and smaller than each of the prime factors $p_1, \ldots, p_f$, and wherein, for at least one integer value l between 1 and m, g_l or $(-g_l)$ is a quadratic residue of the body of integers modulo n, and wherein, for at least one integer value s between 1 and m, q_s is neither congruent to $g_s \bmod n$ nor congruent to $(-g_s) \bmod n$, wherein, for $i = 1, \ldots, m$, $q_i \equiv Q_i^{-v/2} \bmod n$ in the case $G_i \times Q_i^v = 1 \bmod n$ and $q_i = Q_i^{v/2} \bmod n$ in the case $G_i = Q_i^v \bmod n$; and

using at least the private values $Q_1, Q_2, \ldots, Q_m$ in an authentication or in a signature method.

20. (New) The computer-implemented process according to claim 19, further comprising:

receiving a commitment R from a demonstrator, the commitment R having a value computed such that: $R = r^v \bmod n$, wherein r is an integer such that $0 < r < n$ randomly chosen by the demonstrator;

selecting m challenges $d_1, d_2, ..., d_m$ randomly;

sending the challenges $d_1, d_2, ..., d_m$ to the demonstrator;

receiving a response D from the demonstrator, the response D having a value computed such that: $D = r \times Q_1^{d_1} \times Q_2^{d_2} \times ... \times Q_m^{d_m} \bmod n$; and

determining that the demonstrator is authentic if the response D has a value such that: $D^v \times G_1^{\varepsilon_1 d_1} \times G_2^{\varepsilon_2 d_2} \times ... \times G_m^{\varepsilon_m d_m} \bmod n$ is equal to the commitment R, wherein, for $i = 1, ..., m$, $\varepsilon_i = +1$ in the case $G_i \times Q_i^v = 1 \bmod n$ and $\varepsilon_i = -1$ in the case $G_i = Q_i^v \bmod n$.

21. (New) The computer-implemented process according to claim 19, further comprising:

receiving a commitment R from a demonstrator, the commitment R having a value computed using the Chinese remainder method from a set of commitment components R_j wherein $j = 1, ..., f$, each commitment component R_j having a value such that $R_j = r_j^v \bmod p_j$, wherein r_j is an integer such that $0 < r_j < p_j$ randomly chosen by the demonstrator;

selecting m challenges $d_1, d_2, ..., d_m$ randomly;

sending the challenges $d_1, d_2, ..., d_m$ to the demonstrator;

receiving a response D from the demonstrator, the response D being computed from a set of response components D_j using the Chinese remainder method, the response components D_j having a value such that: $D_j = r_j \times Q_{1,j}^{d_1} \times Q_{2,j}^{d_2} \times ... \times Q_{m,j}^{d_m} \bmod p_j$ for $j = 1, ..., f$, wherein $Q_{i,j} = Q_i \bmod p_j$ for $i = 1, ..., m$ and $j = 1, ..., f$; and

determining that the demonstrator is authentic if the response D has a value such that: $D^v \times G_1^{\varepsilon_1 d_1} \times G_2^{\varepsilon_2 d_2} \times ... \times G_m^{\varepsilon_m d_m} \bmod n$ is equal to the commitment R, wherein, for $i = 1, ..., m$, $\varepsilon_i = +1$ in the case $G_i \times Q_i^v = 1 \bmod n$ and $\varepsilon_i = -1$ in the case $G_i = Q_i^v \bmod n$.

22. (New) The computer-implemented process according to claim 19, further comprising:

receiving a token T from a demonstrator, the token T having a value such that

$T = h(M, R)$, wherein h is a function of two integers which makes use of a hash function, M is a message received from the demonstrator, and R is a commitment having a value computed such that: $R = r^v \bmod n$, wherein r is an integer such that $0 < r < n$ randomly chosen by the demonstrator;

selecting m challenges $d_1, d_2, ..., d_m$ randomly;

sending the challenges $d_1, d_2, ..., d_m$ to the demonstrator;

receiving a response D from the demonstrator, the response D having a value such that: $D = r \times Q_1^{d_1} \times Q_2^{d_2} \times ... \times Q_m^{d_m} \bmod n$; and

determining that the message M is authentic if the response D has a value such that: $h\left(M, D^v \times G_1^{\varepsilon_1 d_1} \times G_2^{\varepsilon_2 d_2} \times ... \times G_m^{\varepsilon_m d_m} \bmod n\right)$ is equal to the token T, wherein, for $i = 1,...,m$, $\varepsilon_i = +1$ in the case $G_i \times Q_i^v = 1 \bmod n$ and $\varepsilon_i = -1$ in the case $G_i = Q_i^v \bmod n$.

23. (New) The computer-implemented process according to claim 19, further comprising:

receiving a token T from a demonstrator, the token T having a value such that: $T = h(M, R)$, wherein h is a function of two integers which makes use of a hash function, M is a message received from the demonstrator, and R is a commitment having a value computed using the Chinese remainder method from a set of commitment components R_j wherein $j = 1,...,f$, each commitment component R_j having a value such that $R_j = r_j^v \bmod p_j$, wherein r_j is an integer such that $0 < r_j < p_j$ randomly chosen by the demonstrator;

selecting m challenges $d_1, d_2, ..., d_m$ randomly;

sending the challenges $d_1, d_2, ..., d_m$ to the demonstrator;

receiving a response D from the demonstrator, the response D being computed from a set of response components D_j using the Chinese remainder method, the response components D_j having a value such that: $D_j = r_j \times Q_{1,j}^{d_1} \times Q_{2,j}^{d_2} \times ... \times Q_{m,j}^{d_m} \bmod p_j$ for $j = 1,...,f$, wherein $Q_{i,j} = Q_i \bmod p_j$ for $i = 1,...,m$ and $j = 1,...,f$; and

determining that the message M is authentic if the response D has a value such that: $h\left(M, D^v \times G_1^{\varepsilon_1 d_1} \times G_2^{\varepsilon_2 d_2} \times \ldots \times G_m^{\varepsilon_m d_m} \bmod n\right)$ is equal to the token T, wherein, for $i = 1,\ldots,m$, $\varepsilon_i = +1$ in the case $G_i \times Q_i^v = 1 \bmod n$ and $\varepsilon_i = -1$ in the case $G_i = Q_i^v \bmod n$.

24. (New) The computer-implemented process according to claim 20, wherein the challenges are such that $0 \le d_i \le 2^k - 1$ for $i = 1,\ldots,m$.

25. (New) A computer-implemented process according to claim 19 for allowing a signatory to sign a message M, further comprising:

selecting randomly m integers r_i such that $0 < r_i < n$ for $i = 1,\ldots,m$;

computing commitments R_i having a value such that: $R_i = r_i^v \bmod n$ for $i = 1,\ldots,m$;

computing a token T having a value such that $T = h(M, R_1, R_2, \ldots, R_m)$, wherein h is a function of $(m+1)$ integers which makes use of a hash function and produces a binary train consisting of m bits;

identifying the bits $d_1, d_2, \ldots, d_m$ of the token T; and

computing responses $D_i = r_i \times Q_i^{d_i} \bmod n$ for $i = 1,\ldots,m$.

26. (New) The computer-implemented process according to claim 25, further comprising:

collecting the token T and the responses D_i for $i = 1,\ldots,m$; and

determining that the message M is authentic if the response D has a value such that: $h\left(M, D_1^v \times G_1^{\varepsilon_1 d_1} \bmod n, D_2^v \times G_2^{\varepsilon_2 d_2} \bmod n, \ldots, D_m^v \times G_m^{\varepsilon_m d_m} \bmod n\right)$ is equal to the token T, wherein, for $i = 1,\ldots,m$, $\varepsilon_i = +1$ in the case $G_i \times Q_i^v = 1 \bmod n$ and $\varepsilon_i = -1$ in the case $G_i = Q_i^v \bmod n$.

27. (New) A system comprising:

a memory storing a set of instructions; and

a processor coupled to the memory for executing the set of instructions stored in the memory, the instructions including:

obtaining a set of one or more private values $Q_1, Q_2, ..., Q_m$ and respective public values $G_1, G_2, ..., G_m$, each pair of keys (Q_i, G_i) verifying either the equation $G_i \cdot Q_i^v \equiv 1 \bmod n$ or the equation $G_i \equiv Q_i^v \bmod n$, wherein m is an integer greater than or equal to 1, i is an integer between 1 and m, and wherein n is a public integer equal to the product of f private prime factors designated by $p_1, ..., p_f$, at least two of these prime factors being different from each other, wherein f is an integer greater than 1, and wherein v is a public exponent such that $v = 2^k$, wherein k is a security parameter having an integer value greater than 1, and wherein each public value G_i (for $i = 1, ..., m$) is such that $G_i \equiv g_i^2 \bmod n$, wherein g_i (for $i = 1, ..., m$) is a base number having an integer value greater than 1 and smaller than each of the prime factors $p_1, ..., p_f$, and wherein, for at least one integer value l between 1 and m, g_l or $(-g_l)$ is a quadratic residue of the body of integers modulo n, and wherein, for at least one integer value s between 1 and m, q_s is neither congruent to $g_s \bmod n$ nor congruent to $(-g_s) \bmod n$, wherein, for $i = 1, ..., m$, $q_i \equiv Q_i^{-v/2} \bmod n$ in the case $G_i \times Q_i^v = 1 \bmod n$ and $q_i = Q_i^{v/2} \bmod n$ in the case $G_i = Q_i^v \bmod n$; and

using at least the private values $Q_1, Q_2, ..., Q_m$ in an authentication or in a signature method.

28. (New) A computer-readable storage medium storing instructions which when executed cause a processor to execute the following acts:

obtaining a set of one or more private values $Q_1, Q_2, ..., Q_m$ and respective public values $G_1, G_2, ..., G_m$, each pair of keys (Q_i, G_i) verifying either the equation $G_i \cdot Q_i^v \equiv 1 \bmod n$ or the equation $G_i \equiv Q_i^v \bmod n$, wherein m is an integer greater than or equal to 1, i is an integer

between 1 and m, and wherein n is a public integer equal to the product of f private prime factors designated by $p_1,...,p_f$, at least two of these prime factors being different from each other, wherein f is an integer greater than 1, and wherein v is a public exponent such that $v = 2^k$, wherein k is a security parameter having an integer value greater than 1, and wherein each public value G_i (for $i = 1,...,m$) is such that $G_i \equiv g_i^2 \bmod n$, wherein g_i (for $i = 1,...,m$) is a base number having an integer value greater than 1 and smaller than each of the prime factors $p_1,...,p_f$, and wherein, for at least one integer value l between 1 and m, g_l or $(-g_l)$ is a quadratic residue of the body of integers modulo n, and wherein, for at least one integer value s between 1 and m, q_s is neither congruent to $g_s \bmod n$ nor congruent to $(-g_s) \bmod n$, wherein, for $i = 1,...,m$, $q_i \equiv Q_i^{-v/2} \bmod n$ in the case $G_i \times Q_i^v = 1 \bmod n$ and $q_i = Q_i^{v/2} \bmod n$ in the case $G_i = Q_i^v \bmod n$; and

using at least the private values $Q_1, Q_2,..., Q_m$ in an authentication or in a signature method.

29. (New) A computer-implemented process for producing asymmetric cryptographic keys, said keys comprising $m \geq 1$ private values $Q_1, Q_2,..., Q_m$ and m respective public values $G_1, G_2,..., G_m$, the computer-implemented process comprising:

selecting a security parameter k, wherein k is an integer greater than 1;

determining a modulus n, wherein n is a public integer equal to the product of at least two prime factors $p_1,...,p_f$;

selecting m base numbers $g_1, g_2,..., g_m$, wherein each base number g_i (for $i = 1,...,m$) has an integer value greater than 1 and smaller than each of the prime factors $p_1,...,p_f$, and wherein, for at least one integer value l between 1 and m, g_l or $(-g_l)$ is a quadratic residue of the body of integers modulo n;

calculating the public values G_i for $i = 1,...,m$ through $G_i \equiv g_i^2 \bmod n$; and

calculating the private values Q_i for $i = 1,\ldots,m$ by solving either the equation $G_i \cdot Q_i^v \equiv 1 \bmod n$ or the equation $G_i \equiv Q_i^v \bmod n$, wherein the public exponent v is such that $v = 2^k$, such that, for at least one integer value s between 1 and m, q_s is neither congruent to $g_s \bmod n$ nor congruent to $(-g_s) \bmod n$, wherein, for $i = 1,\ldots,m$, $q_i \equiv Q_i^{-v/2} \bmod n$ in the case $G_i \times Q_i^v = 1 \bmod n$ and $q_i = Q_i^{v/2} \bmod n$ in the case $G_i = Q_i^v \bmod n$.